REMARKS

I. Introduction

In response to the Office Action dated July 26, 2007, claims 18 and 51 have been cancelled, claims 1 and 17 have been amended, and new claims 52 and 53 have been added. Claims 1, 2, 4-17, 19-29, 31-50, 52 and 53 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. Related Cases

The Applicants have amended the specification to cite a number of related cases that were filed subsequent to the instant application. The Applicants have endeavored to cite all of the art from each of these related cases in the instant case, but respectfully ask that Examiner review the file wrapper in these cases for arguments related to patentability and to assess any potential double patenting rejections.

III. Claim Amendments

Applicants' attorney has made amendments to the claims as indicated above. The Applicants are not conceding in this application that those claims are not patentable over the art cited by the Examiner, as the present claim amendments and cancellations are only for clarifying the language of the claims and facilitating expeditious prosecution of the allowable subject matter noted by the examiner. Applicants respectfully reserve the right to pursue these and other claims in one or more continuations and/or divisional patent applications.

IV. The Cited References and the Subject Invention

A. The Okabe Reference

U.S. Patent No. 6,889,208, issued May 3, 2005 to Okabe et al. disclose contents sale system. In the contents sale system, original contents data are encrypted into encryption-resultant contents data in response to original playback key data. The original playback key data are encrypted into first encryption-resultant playback key data. The first encryption-resultant playback key data are encrypted into second encryption-resultant playback key data in response to an ID of a sale

destination terminal apparatus. The encryption-resultant contents data and the second encryption-resultant playback key data are transmitted to the sale destination terminal apparatus. The sale destination terminal apparatus is enabled to decrypt the second encryption-resultant playback key data into the first encryption-resultant playback key data in response to the ID of the sale destination terminal apparatus. The sale destination terminal apparatus is enabled to decrypt the first encryption-resultant playback key data into the original playback key data. The sale destination terminal apparatus is enabled to decrypt the encryption-resultant contents data into the original contents data in response to the original playback key data.

B. The Downs Reference

U.S. Patent No. 6,574,609, issued June 3, 2003 to Downs et al. discloses a method of managing content data and associated metadata. According to the method, the content data and the associated metadata are generated. The content data is transferred to a content host, and the metadata and usage condition data for the associated content are transferred to an electronic store. The metadata and/or the usage condition data are altered in order to form promotional data, and the promotional data is transferred from the electronic store to a customer's system. In one preferred method, the content data is encrypted with a first encrypting key before being transferred to the content host. The first encrypting key is encrypted with a second encrypting key, and the encrypted first encrypting key is transferred along with the metadata and usage condition data to the electronic store. Additionally, the encrypted first encrypting key is transferred along with the promotional data to the customer's system.

C. The Dolphin Reference

U.S. Patent No. 5,677,953, issued October 14, 1997 to Dolphin discloses a system and method for access control for portable data storage media that is said to provide the support of high density removable media, such as CD-ROM or MO, to be used as a distributed media for storing data where access thereto is securely restricted. The secure periodic distribution of several different sets of data information to the end user is said to be achieved with access control selectively performed by at the user's site through communication with the billing/access center. User billing is based on the purchase of the decryption access codes as indicated by the access code attributes

encoded on the media. Access code availability is further controlled by selectively providing for updates of decryption access codes.

D. The Akins Reference

U.S. Patent No. 6,560,340, issued May 6, 2003 to Akins et al. disclose a method and apparatus for geographically limiting service in a conditional access system. A cable television system includes a headend from which service "instances", or programs, are broadcast and a plurality of set top units for receiving the instances and selectively decrypting the instances for display to system subscribers. The service instances are encrypted using public and/or private keys provided by service providers or central authorization agents. Keys used by the set tops for selective decryption may also be public or private in nature, and such keys may be reassigned at different times to provide a cable television system in which piracy concerns are minimized.

V. Office Action Prior Art Rejections

In paragraphs (5)-(6), the Office Action rejected claims 1, 5, 14-18, 20, 25-28, 32, 34, 36, 40-43, and 51 under 35 U.S.C. § 103(a) as being unpatentable over Okabe et al., U.S. Patent No. 6,889,208 (Okabe). Applicants respectfully traverse these rejections.

With Respect to Claim 1: Claim 1 has been amended to recite the features of previously entered claim 51. As amended, claim 1 recites:

> A method of storing program material in a media storage device communicatively coupled to a receiver for subsequent replay, comprising the steps of:
>
> (a) accepting encrypted access control information and the program material encrypted according to a first encryption key in the receiver, the access control information including a first encryption key and control data;
>
> (b) decrypting the received access control information in a conditional access module releasably coupleable with the receiver to produce the first encryption key;
>
> (c) decrypting the program material in the receiver using the first encryption key;
>
> (d) re-encrypting the program material according to a second encryption key;
>
> (e) encrypting the second encryption key in the conditional access module according to a third encryption key to produce a fourth encryption key; and
>
> (f) providing the re-encrypted program material and the fourth encryption key for storage external to the conditional access module.

Claim 1 recites a system that uses a receiver and a conditional access module that is releasably coupled to the receiver. Such systems are common in satellite television applications.

The Applicant's invention differs from the related prior art that the Applicant is aware of in that it encrypts the second (CP) encryption key in the conditional access module instead of the receiver, and does so using an key (CAM key) that is generated or stored internal to the CAM. This implementation is beneficial in that it reduces the benefit that may be derived by hacker from monitoring the CAM/receiver interface.

The Downs reference discloses a system wherein electronic content is transmitted to a user computer. All of the described activities take place in the user's computer. There is no notion receiver and a separate conditional access module at all ... all of the described functionality occurs in the user's computer.

The Okabe reference discloses a system in which electronic content is transmitted to a kiosk, where it can be downloaded into a user's player (and later, to other user's players). Okabe likewise does not use a separate receiver and conditional access module, although the Office Action analogizes the Applicant's receiver and removable CAM to Okabe's terminal and player, respectively.

Claim 1 allocates functions between the receiver in the CAM. Namely, it specifies that:

The conditional access module:

- decrypts the received access control information to produce a key that is used to decrypt the program material
- re-encrypts the program material using a second key;
- re-encrypts the second key using third key to produce a fourth key

The conditional access module does not:

- store the re-encrypted program material and the fourth encryption key; and

The receiver:

- accepts the encrypted access control information and the encrypted program material

Returning to the cited references, we note that Downs discloses no functional allocation between hardware elements at all ... all functions are performed by the user's computer. That certainly does not disclose the functional allocation described in claim 1.

Okabe is of no help. As described below, it discloses a system in which the terminal (which the Office Action analogizes to the Applicant's receiver) receives encrypted playback key and encrypted program material, further encrypts the program key, and transmits the encrypted program material and the further encrypted program key to the player (which the Office Action analogizes to the Applicant's CAM).

> A customer's player 6*a* can be connected to the terminal apparatus 5 via an IEEE1394 interface. The player 6*a* includes a computer which operates in accordance with a control program stored in a memory. The control program is designed to enable the player 6*a* to implement processes mentioned later. The player 6*a* also includes a storage unit. A predetermined ID (a predetermined identification code word) is assigned to the player 6*a*. In the case where the player 6*a* is connected with the terminal apparatus 5, the player 6*a* informs the terminal apparatus 5 of its own ID before downloading. The terminal apparatus 5 separates the composite data into the primary encryption-resultant playback key data and the encryption-resultant contents data. The terminal apparatus 5 encrypts the primary encryption-resultant playback key data into secondary encryption-resultant playback key data (second encryption-resultant playback key data). In the case where the terminal apparatus 5 is connected with the player 6*a*, the terminal apparatus 5 downloads the encryption-resultant contents data and the secondary encryption-resultant playback key data into the storage unit of the player 6*a*. The player 6*a* recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6*a* generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player.

These functions are not analogous those recited in claim 1 (where nothing is "further encrypted", but rather, decrypted and re-encrypted). The player (CAM) decrypts the encrypted content, but does not store that re-encrypted program material or another key for storage external to the player (CAM) as recited in the last step of claim 1. Instead, it stores it internally.[1]

[1] Storage in a second player does not cure this defect, since what is stored in the second player is not the re-encrypted program material and the fourth encryption key that was recited in the preceding step.

Accordingly, even when combined, the Downs an Okabe references do not disclose or teach all of the features of claim 1.

It would also not be obvious to modify the Okabe and Downs combination to arrive at the Applicant's invention. One might be tempted to consider that the Applicant's functional allocation is a simple matter of design choices within the realm of one of ordinary skill in the art. However, this is not the case. As a threshold matter, the prior art teaches a different functional allocation than that which is claimed by the Applicants.

Consider the system described in EP 0 989 557 A1 (hereinafter, "EP" system), for example. Unlike either of the references relied upon in rejecting the Applicants' claims, this reference discloses a receiver used in conjunction with a removable CAM, and teaches that the second encryption key is encrypted in the receiver, not the CAM.

Both systems same the same ultimate goal ... to minimize the possibility of compromising the security of the stored media program ... but only the Applicant's invention achieves it.

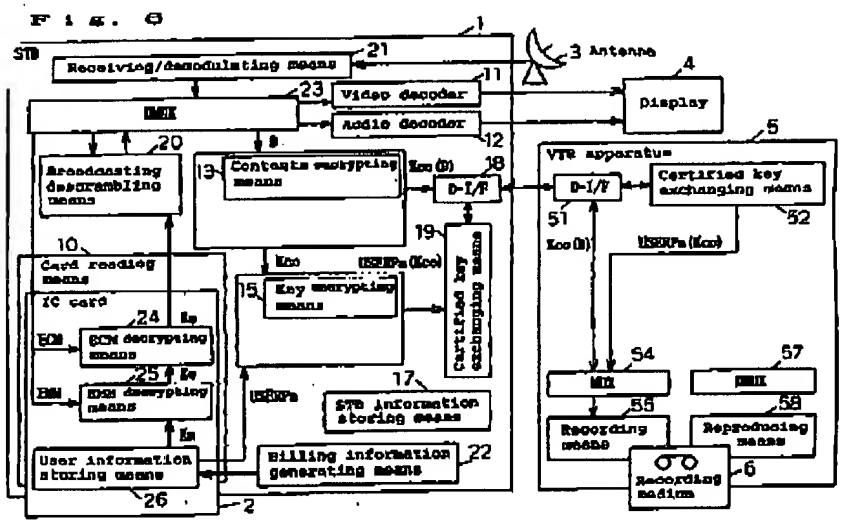
The EP system describes the storage of the USERPa key on a smart card that is coupled to an STB before use. Smart cards are well known in the art to include a plurality of electrical connectors that mate with matching connectors in a card reader when the card is inserted into the reader. The EP system discloses such a reader (the card reading means 10). The Applicant's invention also discloses the use of a conditional access module that is coupled to the receiver before use:

> The IRD 132 is communicatively coupleable to a conditional access module (CAM) 406. The CAM 406 is typically implemented in a smart card or similar device, which is provided to the subscriber 110 to be inserted into the IRD 132.

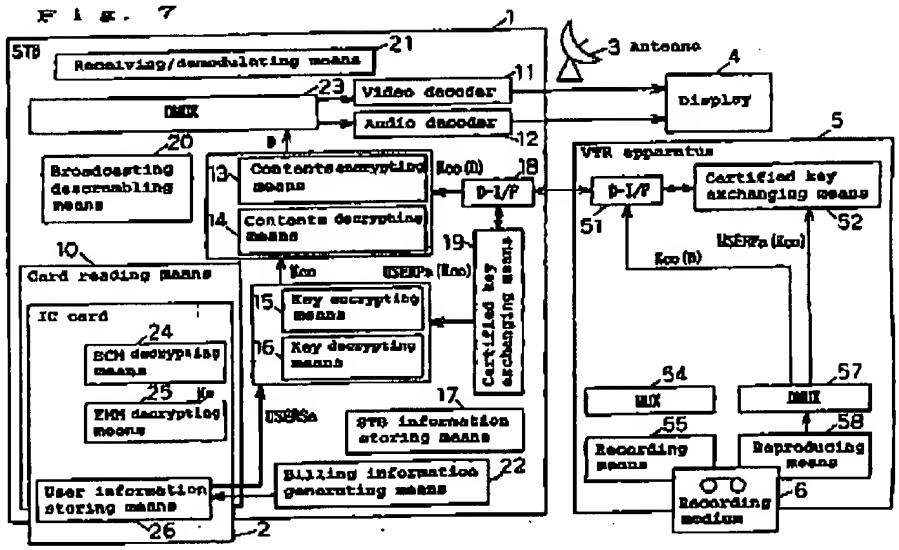
Because the CAM is communicatively coupled to the receiver by the subscriber by inserting it into the receiver, the Applicant's invention is subject to the same problem as the EP system ... the signals passing to and from the CAM may be monitored. In embodiments where the CAM is a smart card (like the EP system), this involves simply monitoring the electrical connectors of the smart card.

Referring to FIG. 6a, below, the EP system transmits a USERPa (user public) key from the smart card to the STB in unencrypted form. The EP system then encrypts the program material

with a Kco key, encrypts that Kco key with the USERPa key obtained from the smart card (thus generating USERPa(Kco)), and stores both in the recording medium.



Note that the Kco key cannot be easily monitored by monitoring the link between the contents encrypting means and the key encrypting means (since that is internal to the STB and not passed from the STB to the IC card. However, the unencrypted USERPa key can be monitored directly from on the smart card, leaving it open to compromise. The user's secret key is needed to decrypt the media program as described in FIG. 7 below:



Note that the user's secret key USERSa can also be monitored directly from the smart card, leaving it open to compromise as well.

Also note that the ultimate security of the EP system depends on the user's secret key. If that key is compromised, it can always be used to determine Kco (even if it is time-invariant), and any program material stored in the recording medium 6 can be recovered. In other words, to defeat the entire system, the pirate need only determine the value of USERSa, and that value is not difficult to obtain.

The Applicant's invention encrypts the CP (presumably analogous to Kco) within the CAM instead of the receiver, as shown below:

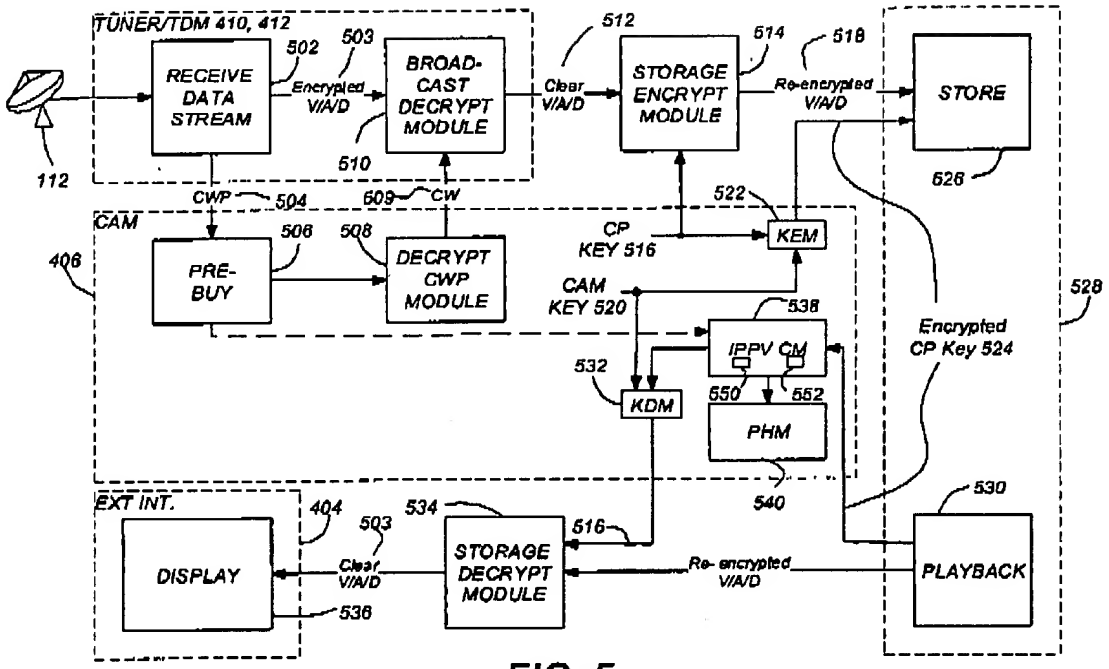


FIG. 5

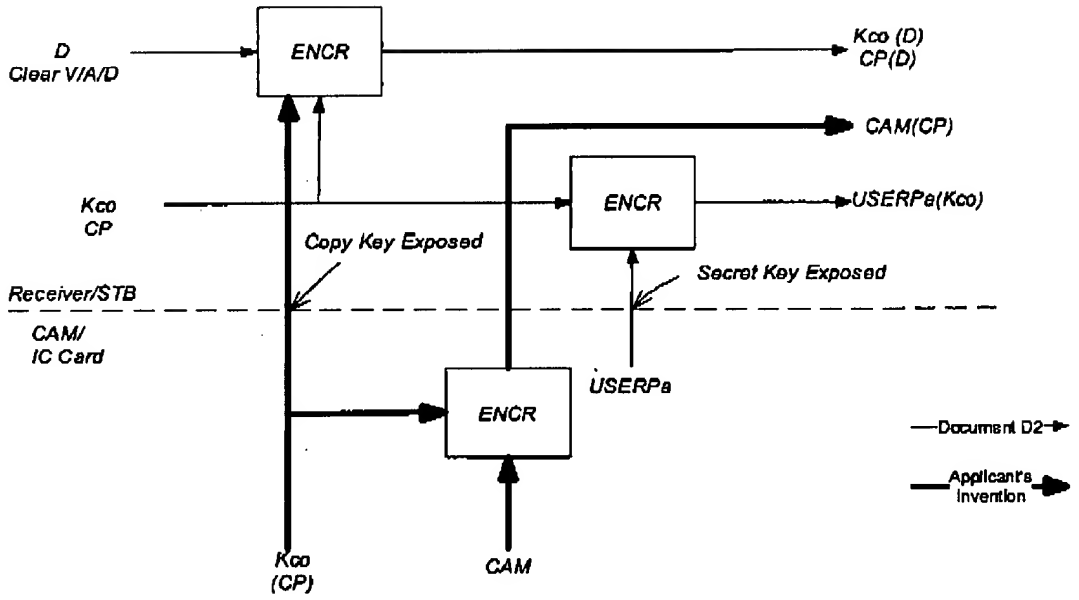
By doing so, the CP key is exposed, because it is passed unencrypted from the CAM to the receiver.[2] However, the CAM key (perhaps analogous to the USERPa or USERSa key) is never exposed. It is always encrypted before leaving the CAM.

This difference is significant. The EP system is less secure because it exposes the heart of it's security (USERSa) by passing it unencrypted from the IC card to the receiver. Once the hacker has gained access to the value of USERSa, they can decrypt *any* program that was stored on the storage medium. Further, since USERSa does not change over time, the hacker need not concern themselves with regenerating a new USERSa over time. It need only be accomplished once.

Contrast this with the Applicant's invention. Because the Applicant's invention exposes the copy protection key CP (perhaps analogous to Kco), but not the CAM key, the Applicant's invention is somewhat vulnerable to a hacker trying obtain the value of CP key, but invulnerable to a hacker attempting to divine the value of the CAM key. This is shown diagrammatically below:

---

2 It may be possible to encrypt this information from the CAM and decrypt it in the receiver, but this additional capability would increase the cost of both the STB and the CAM.



The Applicant's solution is especially well suited to systems wherein the value of the CP key changes over time or changes with the media program. That's because a compromise of the CP key will only allow the hacker to view one program or only a portion of one program. Unlike the EP system, what is compromised does not permit the hacker to view *all* programs.

Finally, the Office Action offers the following motivation to combine the Okabe and Downs references:

> It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of protecting digital content used in distribution taught in '208 to include a controlling the number of copies generated. One of ordinary skill in the art would have been motivated to perform such a modification because content distributors have been slow to embrace digital content distributions systems because of the lack of security for digital content see '609 (col. 2, lines 2-44) "The use of global distribution systems such as the Internet for distribution of digital assets such as music, film, computer programs, pictures, games and other content continues to grow. At the same time owners and publishers of valuable digital content have been slow to embrace the use of the Internet for distribution of digital assets for several reasons. One reason is that owners are afraid of unauthorized copying or pirating of digital content. The electronic delivery of digital content removes several barriers to pirating . . . This degradation in quality is not present when a picture is stored digitally. Each copy, and every generation of copies can be as clear and crisp as the

original. The aggregate effect of perfect digital copies combined with the very low cost to distribute content electronically and to distribute content widely over the Internet makes it relatively easy pirate and distribute unauthorized copies. With a couple of keystrokes, a pirate can send hundred or even of thousands of perfect copies of digital content over the Internet. Therefore a need exists to ensure the protection and security of digital assets distributed electronically. Providers of digital content desire to establish a secure, global distribution system for digital content that protects the rights of content owners. The problems with establishing a digital content distribution system includes developing systems for digital content electronic distribution, rights management, and asset protection".

This provides a generalized motivation to provide for digital rights (something that both Okabe and Downs provide already provide individually), but does not explain why one would modify Okabe as described in Downs or Downs as described in Okabe. Accordingly it does not make out a prima facie case for obviousness.

For all of the foregoing reasons, the Applicants respectfully traverse the rejection of claim 1.

Claims 17 and 28 recite features analogous to those of claim 1, and are patentable for the same reasons.

With Respect to Claim 25: Claim 25 recites that the second key is stored in the conditional access module. According to the Office Action, this feature is disclosed as follows:

> A customer's player 6*a* can be connected to the terminal apparatus 5 via an IEEE1394 interface. The player 6*a* includes a computer which operates in accordance with a control program stored in a memory. The control program is designed to enable the player 6*a* to implement processes mentioned later. The player 6*a* also includes a storage unit. A predetermined ID (a predetermined identification code word) is assigned to the player 6*a*. In the case where the player 6*a* is connected with the terminal apparatus 5, the player 6*a* informs the terminal apparatus 5 of its own ID before downloading. The terminal apparatus 5 separates the composite data into the primary encryption-resultant playback key data and the encryption-resultant contents data. The terminal apparatus 5 encrypts the primary encryption-resultant playback key data into secondary encryption-resultant playback key data (second encryption-resultant playback key data). In the case where the terminal apparatus 5 is connected with the player 6*a*, the terminal apparatus 5 downloads the encryption-resultant contents data and the secondary encryption-resultant playback key data into the storage unit of the player 6*a*. The player 6*a* recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player 6*a* generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player.

The second key is the key used to re-encrypt the decrypted program material. Player 6a, which the Office Action appears to analogize to the CAM, does not store a second key used to re-encrypt decrypted program material. Accordingly, the Applicants traverse the rejection of claim 25.

In paragraph (7), the Office Action rejected claims 2, 4, 29, and 31 under 35 U.S.C. §103(a) as being unpatentable over Okabe in view of Downs et al., U.S. Patent No. 6,574,609 (Downs) in further view of Dolphin, U.S. Patent No. 5,677,953 (Dolphin). Applicants respectfully traverse these rejections for the reasons described above with respect to the independent claims the foregoing claims depend upon.

In paragraph (8), the Office Action rejected claims 6-13, 19, 21-24, 33, 35, 37-39, and 44-50 under 35 U.S.C. §103(a) as being unpatentable over Okabe in view of Downs in further view of Akins, III et al., U.S. Patent No. 6,560,340 (Akins). Applicants respectfully traverse these rejections.

With Respect to Claims 6, 44-50: Claim 6 recites that the second encryption key is generated at least in part from the metadata. According to the Office Action, this feature is disclosed in the Akins reference as follows.

> instance 105. Control word 117 is produced by control word generator 119 from information contained in entitlement control message 107 and information from authorization information 121 stored in set-top box 113. For example, authorization information 121 may include a key for the service and an indication of what programs in the service the subscriber is entitled to watch. If the authorization information 121 indicates that the subscriber is entitled to watch the program of encrypted instance 105, control word generator 119 uses the key together with information from ECM 107 to generate control word 117. Of course, a new control word is generated for each new ECM 107.

Respectfully, this only discloses the use of a control word to determine whether the subscriber is entitled to view a program. It does not even remotely disclose generating the second encryption key at least in part from metadata. Further, the motivation to modify Okabe and Downs as described in Akins (more flexibility) doesn't explain how any suggested change would increase flexibility.

There is a significant advantage in generating the second key at least in part from the metadata. It prevents having to generate a random number for the second key, and also assures that the metadata can be later recovered. That recovered metadata can be simply used to control replay or can be compared to the metadata before encryption to assure that the second key has not been

tampered with. None of these advantages is even remotely suggested by any of the cited references. Claim 44 recites similar features and is patentable for the same reasons.

Claim 45 recites that the second encryption key is augmented with a least a portion of the metadata before encrypting the second encryption key in the CAM. According to the Office Action, this is disclosed as described above. The Applicants respectfully disagree for the reasons described above, and because the above passage further does not disclose augmenting a key with metadata before encryption. Claim 46 is patentable for analogous reasons.

Claims 47-50 recite analogous features to those above, and are patentable for the same reasons.

With Respect to Claim 13: Claim 13 recites:

> The method of claim 12, wherein steps (b)-(f) are performed in response to a pre-buy message, and wherein:
>
> the second encryption key and the third encryption key are stored in a smartcard, and the replay right data is generated from the metadata and the pre-buy message in the smartcard; and
>
> the steps of accepting the buy data, comparing the buy data with the replay right data, and decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data and the replay right data are performed in the smartcard.

None of the cited references discloses the functional allocation presented in claim 13.

VI. Dependent Claims

Dependent claims 2, 4-16, 18-27, 29, and 31-51 incorporate the limitations of their related independent claims, and are therefore patentable on this basis. In addition, these claims recite novel elements even more remote from the cited references. Accordingly, the Applicants respectfully request that these claims be allowed as well.

VII. New Claims

New claims 52 and 53 are presented for the first time in this Amendment. For the reasons described above, particularly with respect to claim 25, new claims 52 and 53 are patentable over the prior art of record, and the Applicants respectfully request the allowance of these claims as well.

VIII. Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

Date: October 26, 2007

By: _____
Name: Victor G. Cooper
Registration No.: 39,641
Attorney for Applicant

The DIRECTV Group, Inc.
CA / LA1 / A109
2230 E. Imperial Highway
P. O. Box 956
El Segundo CA 90245-0956

Telephone No.: (310) 964-0735